
Article:
Cumanan, Kanapathippillai orcid.org/0000-0002-9735-7019, Zhang, Miao, Thiyagalingam, Jeyarajan et al. (4 more authors) (2021) Exploiting Deep Learning for Secure Transmission in an Underlay Cognitive Radio Network. IEEE Transactions on Vehicular Technology. pp. 726-741. ISSN 0018-9545

https://doi.org/10.1109/TVT.2021.3050104

Exploiting Deep Learning for Secure Transmission in an Underlay Cognitive Radio Network

Miao Zhang, *Member, IEEE,* Kanapathippillai Cumanan, *Senior Member, IEEE,* Jeyarajan Thiyagalingam, *Senior Member, IEEE,* Yanqun Tang, Wei Wang, *Member, IEEE,* Zhiguo Ding, *Fellow, IEEE,* and Octavia A. Dobre, *Fellow, IEEE*

***Abstract*—This paper investigates a machine learning-based power allocation design for secure transmission in a cognitive radio (CR) network. In particular, a neural network (NN)-based approach is proposed to maximize the secrecy rate of the secondary receiver under the constraints of total transmit power of secondary transmitter, and the interference leakage to the primary receiver, within which three different regularization schemes are developed. The key advantage of the proposed algorithm over conventional approaches is the capability to solve the power allocation problem with both perfect and imperfect channel state information. In a conventional setting, two completely different optimization frameworks have to be designed, namely the robust and non-robust designs. Furthermore, conventional algorithms are often based on iterative techniques, and hence, they require a considerable number of iterations, rendering them less suitable in future wireless networks where there are very stringent delay constraints. To meet the unprecedented requirements of future ultra-reliable low-latency networks, we propose an NN-based approach that can determine the power allocation in a CR network with significantly reduced computational time and complexity. As this trained NN only requires a small number of linear operations to yield the required power allocations, the approach can also be extended to different delay sensitive applications and services in future wireless networks. When evaluate the proposed method versus conventional approaches, using a suitable test set, the proposed approach can achieve more than 94% of the secrecy rate performance with less than 1% computation time and more than 93% satisfaction of interference leakage constraints. These results are obtained with significant reduction in computational time, which we believe that it is suitable for future real-time wireless applications.**

***Index Terms*—Deep learning, neural network, physical layer security, cognitive radio networks, resource allocation techniques.**

The work of M. Zhang was supported by the Research Start Up Funding of Chongqing Jiaotong University under grant number 2020020070. The work of Y. Tang was supported by the Guangdong Natural Science Foundation under grant number 2019A1515011622 and the National Natural Science Foundation under grant number 62071499. The work of W. Wang was supported in part by the Six Categories Talent Peak of Jiangsu Province under Grant KTHY-039, the Science and Technology Program of Nantong under Grant MS22019019 and the Verification Platform of Multi-tier Coverage Communication Network for oceans under Grant LZC0020. (*Corresponding author: Yanqun Tang.*)

M. Zhang is with the School of Information Science and Engineering, Chongqing Jiaotong University, Chongqing, China, (email: miao.zhang@cqjtu.edu.cn).

K. Cumanan is with the Department of Electronic Engineering, University of York, York, United Kingdom, YO10 5DD (email: kanapathippillai.cumanan@york.ac.uk).

J. Thiyagalingam is with the Scientific Computing Department of Rutherford Appleton Laboratory, Science and Technology Facilities Council, Harwell Campus, Ditcot, UK (email: t.jeyan@stfc.ac.uk).

Y. Tang is with the School of Information Science and Engineering, Chongqing Jiaotong University, Chongqing, China,also with the School of Electronics and Communication Engineering, Sun Yat-Sen University, Shenzhen, 510006, China (email: tangyq8@mail.sysu.edu.cn)

W. Wang is with the School of Information Science and Technology, Nantong University, Nantong, China, and with the Nantong Research Institute for Advanced Communication Technologies, Nantong, China, and also with Research Center of Networks and Communications, Peng Cheng Laboratory, Shenzhen, China (e-mail: wwang2011@ntu.edu.cn).

Z. Ding is with the School of Electrical and Electronic Engineering, The University of Manchester, Manchester, UK (email: zhiguo.ding@manchester.ac.uk).

O. A. Dobre is with the Department of Electrical and Computer Engineering, Memorial University, St. John's, NL A1B 3X5, Canada (email: odobre@mun.ca).

I. Introduction

Wireless communications have become an indispensable part of daily life of people as they play a crucial role in our day-to-day activities and the means of interactions in the current networked society. However, information security is one of the major challenges in wireless networks due to the open nature of wireless signal transmission which is more vulnerable for interception and eavesdropping. The conventional security methods employed at upper layers in the current communication systems completely rely on cryptographic techniques [1], [2]. Despite the fact that existing conventional security techniques, developed based on some high complex intractable mathematical problems, are difficult to break or intercept, the broadcast nature of wireless transmissions introduces different challenges in terms of secret key exchange and distributions [3], [4]. As a result, information theoretic based physical layer security has been proposed to complement the conventional cryptographic methods and to provide additional security measures in wireless transmissions. Furthermore, this approach exploits the dynamics of physical layer characteristics of wireless channels to establish secure transmission [1]. A reasonable secrecy rate can be realized through physical layer security technique provided that the signal-to-interference plus noise ratio (SINR) of the channel of the legitimate user is better than that of the channel of the eavesdropper [5]. This novel technique was first theoretically proved by Shannon [5] and then secrecy capacities of wiretap and related channels were developed by Wyner [6] and Csiszar [7]. In contrast to the conventional cryptographic methods, physical layer security schemes are more suitable for practical implementations as these techniques do not require any secret key distributions or exchange. Furthermore, it is difficult for interceptors to decipher the information transmitted across wireless channels based on physical layer security [3].

Recently, machine learning techniques have been applied widely as a solution approach to solve different challenging

problems that have complicated structures with stringent constraints on computational time [8]. Furthermore, artificial intelligence has become one of the fastest growing techniques in many research topics [9] and its practical implementations can be realized through different machine learning techniques. As such, these techniques enable machines to acquire knowledge from their computations and make decisions according to the environment [10]–[12]. There are various machine learning frameworks available in the literature [9]–[13], such as linear regression, logistic regression, and neural network (NN). NN is one of the well-known machine learning technique due to its capabilities to simply realize different relationships in complicated and statistical data sets [14], [15]. In recent years, numerous research interests have been developed to utilize NN to design and optimize wireless communication systems, where the researchers believe that NN will be the core technique for 5G and beyond wireless systems [16]–[19].

A. Motivation and Contributions

In secure transmission designs, different optimization approaches with various approximations techniques have been widely exploited to solve complicated and mathematically intractable resource allocation problems [20]–[25]. However, these techniques often have been developed based on iterative approaches to yield either optimal or sub-optimal solutions. The computational complexities associated with these conventional optimization techniques are neither affordable in low powered devices in Internet-of-Things (IoT) nor suitable for applications with ultra reliability and low latency in future wireless networks. Furthermore, these conventional optimization techniques pose different challenges in delay sensitive systems as the dynamic nature of real-time parameters requires frequent updates in very short time [26]. This introduces different stringent delay requirements in updating those design parameters which is impossible to meet by conventional optimization approaches. Machine learning techniques can be considered as the potential solution approaches to solve these real-time update issues. Among a number of machine learning approaches, the deep learning approach has a number of benefits. Although some of these benefits are shared across different methods, deep learning offers better learn-ability with increased volumes of data. We summarize these benefits as follows:

1) NN has the potential capabilities to provide a solution with a short time frame with reduced computational complexity [27], compared to other machine learning techniques, such as support vector machine (SVM) and Gaussian processes (GP) [27], [28]. A particular advantage here is that conventional machine learning approaches use all available data, whereas the NN relies on samples of data from batches (mini-batch gradient descent algorithm). This process demands only a subset of the available large dataset at each training step, opposed to every data point;
2) A single NN model can be trained to meet the objectives of multiple tasks [27], whereas it is difficult for other machine learning techniques to achieve those multi-objectives with the same model; and
3) Furthermore, NN is able to automatically extract features from the data with highly complex datasets and to formulate the latent representations, which can further help with learning [29].

In the literature, several bodies of work have demonstrated that machine learning techniques can be exploited to solve these types of problems in different real-time wireless communication applications. For example, deep learning-based channel estimation and signal detection techniques in orthogonal frequency division multiplexing (OFDM) systems is investigated in [30]. A deep NN-based method for efficient on-line configuration of reconfigurable intelligent surfaces is proposed in [31], where the transmitted signal focusing is improved under the indoor environment. The deep reinforcement learning based joint transmit beamforming and phase shift matrix design for reconfigurable intelligent surface aided MISO systems is studied in [32]. The NN-based spectrum and energy efficiency maximization techniques is proposed for cognitive radio (CR) network in [33]. A learning-based approach for wireless resource management is presented in [26], whereas a reinforcement learning based resource allocation technique is developed for vehicle-to-vehicle communications in [34]. A deep NN is utilized to learn the interference management over interference-limited channels in [35], whereas the authors design a deep NN for channel calibration between the uplink and downlink directions in generic massive MIMO systems in [36]. However, none of these work have considered employing machine learning techniques to simultaneously solve resource allocation problems with perfect and imperfect channel state information (CSI) in secure communication systems.

In general, the motivations behind this work can be summarized as follows: (1) Although the conventional optimization approaches can yield global or local optimal solutions for resource allocation problems, the nature of their complex implementations render them less practical for real-world deployments, particularly on resource-limited edge devices where tolerance for delays are very minimal. For NNs, once trained, the inference step does not demand back-propagation, at which point it only relies on limited number of floating point arithmetic. This offers a two-fold benefit. First, once trained (using powerful computational resources), the NN model can be moved around for inference purposes, particularly on edge devices where computational resources are often limited. Secondly, an NN-based approach can offer almost near real-time performance. This is clearly evidenced by modern edge devices, such as smart phones and cameras. (2) As NN provides reduced computational complexity for inference compared to other machine learning techniques, it is useful for our resource allocation problem. (3) Finally, with the rise of machine learning algorithms in various domains of sciences, the community would benefit if some baseline performance can be established for resource allocation problems in wireless communications and be compared against conventional optimization-based solutions.

To carry out the study, in this paper, we consider a secure transmission in a CR network problem as shown in Fig. 1. This secure network consists of one primary transmitter (PU-Tx), one primary receiver (PU-Rx), one secondary transmitter

(SU-Tx), one secondary receiver (SU-Rx) and one eavesdropper (EVE). These terminals are equipped with a single antenna. Our main objective is to design an NN approach that can achieve near optimal secrecy rate performances with significantly reduced computational time compared to the existing conventional optimization schemes in the literature. In particular, the optimal power allocation is determined to maximize the achievable secrecy rate under the constraints of total transmit power of the SU-Tx and the interference leakage to the PU-Rx. We develop two approaches in this paper: the conventional optimization approach and NN-based framework. We show that the NN-based approach can be exploited to solve both robust and non-robust secrecy rate maximization problem, whereas the conventional optimization techniques require completely two different problem formulation and solution approaches. Our contributions of this work are summarized as follows:

1) Firstly, to the best of our knowledge and surveys [27], [37], [38], none of the existing work considered developing an NN framework to solve the secrecy rate maximization problems in an underlay CR network.
2) Secondly, due to the imperfections and non-linearities in practical systems [39], we also consider a more practical imperfect CSI scenario in this paper, whereas most of the previous works that apply NN for resource allocation problems only consider the perfect CSI scenarios. Therefore, the framework of the proposed NN is different from those found in related works, i.e., we have added the channel error bounds as input parameters to enable the NN to learn the impact of these errors on the power allocation.
3) Thirdly, we propose an NN-based algorithm to simultaneously solve the secrecy rate maximization problem with perfect and imperfect CSI at the SU-Tx. The key advantage of the developed approach is that the same NN-based algorithm can be exploited to solve both the robust and the non-robust secrecy rate maximization problems with the both imperfect and perfect CSI, respectively. Opposite to that, in the conventional optimization approaches, these problems need to be formulated into two completely different optimization frameworks. Furthermore, to reduce over-fitting, we also embed two regularization techniques into our proposed NN designs. To generate the required training set, we utilize the conventional optimization framework and then train the NN with this training set to determine appropriate weights of the connections in the proposed NN. These weighted connections establish a mathematical relationship between the input and the corresponding output. After completing the training process, we evaluate the performance of the proposed NN-based approach versus the the conventional optimization approaches available in the literature.
4) Finally, we compare the performance of both schemes in terms of achieved secrecy rate and required computation time to demonstrate the effectiveness and superiority of our proposed NN scheme.

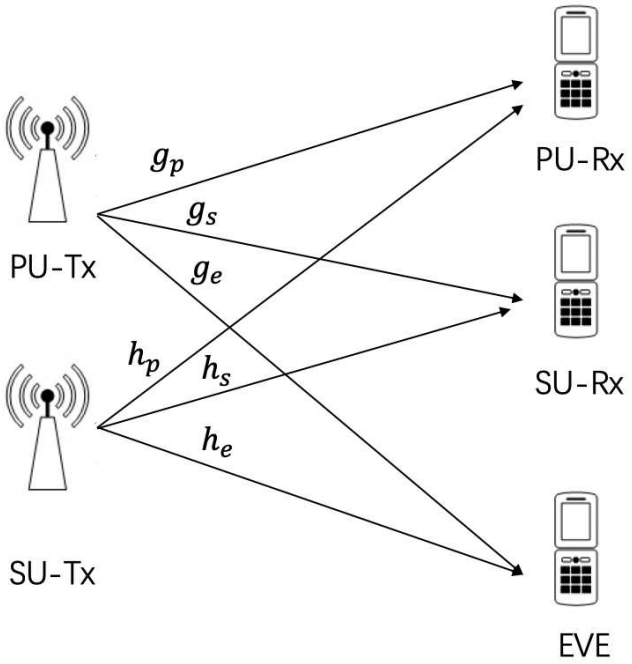

Fig. 1: A CR network with one PU-Tx, one PU-Rx, one SU-Tx, one SU-Rx and one EVE. Each is equipped with a single antenna.

The remainder of this paper is organized as follows. The system model is presented in Section II, whereas the secrecy rate maximization problems with both perfect and imperfect CSI are formulated and solved by using conventional optimization technique in Section III. Section IV presents an NN-based optimization framework. Section V provides simulation results to demonstrate the effectiveness of the proposed approach. Section VI discusses the limitations of the proposed approach and several potential directions for future work, and finally, Section VII concludes this paper.

B. Notations

We use the upper and the lower case boldface letters for matrices and vectors, respectively. $(\cdot)^{-1}$, $(\cdot)^T$ and $(\cdot)^H$ stand for inverse, transpose and conjugate transpose operation, respectively. $|a|$ represents the absolute value of a. $[x]^+$ defines $\max\{x, 0\}$. The 1-norm and 2-norm of x are expressed respectively as $||x||_1$ and $||x||_2$. $\mathbf{A} \cdot \mathbf{B}$ represents the dot product of matrix $\mathbf{A}$ and $\mathbf{B}$. $h^{'}(x)$ is the first derivative of function h at x. The circularly symmetric complex Gaussian distribution with mean μ and variance σ^2 is represented by $\mathcal{CN}(\mu, \sigma^2)$.

II. System Model and Problem Formulation

We consider a CR network as shown in Fig. 1 with five terminals: one PU-Tx, one SU-Tx, one SU-Rx, one PU-Rx and one EVE. All terminals are equipped with single antenna. The SU-Tx intends to send a confidential message to the SU-Rx while ensuring that the interference leakage to the PU-Rx is less than a predefined threshold. At the same time, the EVE attempts intercepting the information sent by the SU-Tx to SU-Rx. The channels between PU-Tx and PU-Rx, SU-Rx, and

EVE are represented by g_p, g_s, and g_e, respectively, whereas the channels between the SU-Tx and PU-Rx, SU-Rx, and EVE are denoted by h_p, h_s, and h_e, respectively. The received signal at the SU-Rx and EVE can be expressed, respectively, as

$$y_s = \sqrt{P_s} h_s x_s + \sqrt{P_p} g_s x_p + n_s, \tag{1}$$

$$y_e = \sqrt{P_s} h_e x_s + \sqrt{P_p} g_e x_p + n_e, \tag{2}$$

where $x_s(\mathbb{E}\{|x_s|^2\} = 1)$ and $x_p(\mathbb{E}\{|x_p|^2\} = 1)$ are the symbols sent from the SU-Tx to SU-Rx and the PU-Tx to PU-Rx, respectively. The noise at the SU-Rx and EVE are denoted by $n_s(\mathbb{E}\{|n_s|^2\} = \sigma_s^2)$ and $n_e(\mathbb{E}\{|n_e|^2\} = \sigma_e^2)$, respectively. Furthermore, P_s and P_p represent the power allocations at the SU-Rx and the EVE, respectively. The SINR at the SU-Rx and EVE are defined as

$$\gamma_s = \frac{P_s |h_s|^2}{P_p |g_s|^2 + \sigma_s^2}, \tag{3}$$

$$\gamma_e = \frac{P_s |h_e|^2}{P_p |g_e|^2 + \sigma_e^2}. \tag{4}$$

The achievable secrecy rate at the SU-Rx can be written as [40]

$$R_s = [\log_2(1+\gamma_s) - \log_2(1+\gamma_e)]^+. \tag{5}$$

The interference leakage to the PU-Rx can be expressed as

$$P_{in} = P_s |h_p|^2. \tag{6}$$

With these definitions, the secrecy rate maximization problem can be formulated as

$$\begin{aligned} \max_{P_s} \quad & R_s \\ s.t. \quad & P_s |h_p|^2 \le q, \\ & P_s \le P_t, P_s \ge 0, \end{aligned} \tag{7}$$

where q is the maximum interference leakage to the PU-Rx, and P_t is the maximum transmit power available at the SU-Tx. In the following sections, we present two ways to solve this problem: conventional optimization approaches and NN-based approach.

III. Conventional Optimization based Power Allocation Approach

In this section, we present conventional convex optimization approaches to solve the secrecy rate maximization problem defined in (7) by taking into account the scenarios of having both perfect and imperfect CSI at the SU-Tx.

A. Perfect CSI

In this subsection, we present the conventional convex optimization-based approach to solve the problem defined in (7) with perfect CSI assumption. The original problem (7) is non-convex in its original form due to the non-convex objective function. Based on the monotonicity of logarithmic functions, we reformulate the original problem in (7) as

$$\begin{aligned} \max_{P_s} \quad & \frac{1 + \frac{P_s |h_s|^2}{P_p |g_s|^2 + \sigma_s^2}}{1 + \frac{P_s |h_e|^2}{P_p |g_e|^2 + \sigma_e^2}} \\ s.t. \quad & P_s |h_p|^2 \le q, \\ & P_s \le P_t, P_s \ge 0. \end{aligned} \tag{8}$$

The above problem still remains non-convex due to the fractional objective function, and therefore, it cannot be directly solved using existing convex optimization tools. To circumvent this non-convexity issue, we convert the original problem into a two-level optimization problem, namely outer problem and inner problem. The outer problem can be written with respect to (w.r.t.) a new scalar variable t as

$$\max_{t \ge 0} \quad \frac{f(t)}{1+t}, \tag{9}$$

whereas the inner problem can be expressed for a given t as

$$\begin{aligned} f(t) = \max_{P_s} \quad & 1 + \frac{P_s |h_s|^2}{P_p |g_s|^2 + \sigma_s^2} \\ s.t. \quad & P_s |h_p|^2 \le q, \\ & \frac{P_s |h_e|^2}{P_p |g_e|^2 + \sigma_e^2} \le t, \\ & P_s \le P_t, P_s \ge 0. \end{aligned} \tag{10}$$

The inner problem in (10) is convex for a given t and can be solved by using standard interior-point methods. Since the inner problem in (10) is a convex problem, the outer problem in (9) is a quasi-convex optimization problem w.r.t. variable t. Therefore, we employ a one-dimensional search to obtain the optimal t^* and P_s^* [41]. The proposed one-dimensional search algorithm is summarized in Algorithm 1.

Algorithm 1 : One-dimensional search based on bisection method

1: Initialize $t \in [0, t_{max}]$, $c = (\sqrt{5}-1)/2$, $a = 0$, $b = t_{max}$, $t_1 = (1-c)b$, $t_2 = cb$;
2: Compute $f(t_1)$, $f(t_2)$;
3: **Repeat**
4: If $\frac{1+f(t_1)}{1+t_1} > \frac{1+f(t_2)}{1+t_2}$, $b = t_2$, $t_2 = t_1$, $f(t_2) = f(t_1)$, $t_1 = a + c(b-a)$ and update $f(t_1)$;
5: Else, $a = t_1$, $t_1 = t_2$, $f(t_1) = f(t_2)$, $t_2 = a + c(b-a)$, and update $f(t_2)$;
6: **Until** $|b-a| \le \epsilon$, where ϵ is threshold to terminate the algorithm.

B. Imperfect CSI

In this subsection, we develop a tractable approach to solve the secrecy rate maximization problem with imperfect CSI available at the SU-Tx. We reformulate this robust problem into a tractable one by exploiting the Charnes-Cooper transformation [42] and S-Procedure [43].

In practical scenarios, it is difficult for SU-Tx to obtain perfect CSI due to the channel estimation and quantization errors [44]. Instead, the SU-Tx has knowledge of its estimated CSI and the uncertainty regions that contain the actual channel realizations, which is referred to imperfect CSI. Note that the imperfect CSI of the PU-Rx and SU-Rx can be estimated based on the standard CSI feedback techniques [45]. Furthermore, the imperfect CSI of EVE can be obtained by the following

two methods: (1) for the case when EVE is part of the system, the CSI can be estimated with the standard CSI feedback techniques, as is still part of the system and should be able to cooperate with SU-TX with its CSI feedback [45]; (2) when EVE is not part of the system, the CSI can be estimated at the SU-Tx through the local oscillator power leakage from the EVE's RF front end, the details of which can be found in [46].

In this work, the imperfect CSI is modelled based on the deterministic models [1], [44], [47], in which it is assumed that the actual channel lies in an ellipsoid centred at the channel mean. In this CSI assumption, the estimated CSI and the error bounds are known at the SU-Tx, while the actual value of channel errors are unknown [1], [44], [47]. The actual channel coefficients can be modelled with corresponding channel uncertainties as follows:

$$h_s = \hat{h}_s + e_s,\ h_e = \hat{h}_e + e_e,\ h_p = \hat{h}_p + e_p, \tag{11}$$

where $\hat{h}_s$, $\hat{h}_e$ and $\hat{h}_p$ are the channel coefficients estimated by the SU-Tx. Furthermore, the symbols $e_s,\ e_e$ and e_p represent the channel uncertainties. These channel uncertainties are assumed to be bounded by a predefined ellipsoids, as follows:

$$|e_s| = |h_s - \hat{h}_s| \leq \epsilon_s, \tag{12}$$

$$|e_e| = |h_e - \hat{h}_e| \leq \epsilon_e, \tag{13}$$

$$|e_p| = |h_p - \hat{h}_p| \leq \epsilon_p, \tag{14}$$

where $\epsilon_s \geq 0$, $\epsilon_e \geq 0$ and $\epsilon_p \geq 0$ are the error bounds. Based on these bounded channel uncertainties and the monotonicity of log functions, the robust secrecy rate maximization problem can be reformulated into the following robust optimization framework:

$$\begin{aligned} \max_{P_s} \quad & \frac{1+\frac{P_s|\hat{h}_s+e_s|^2}{P_p|g_s|^2+\sigma_s^2}}{1+\frac{P_s|\hat{h}_e+e_e|^2}{P_p|g_e|^2+\sigma_e^2}} \\ s.t. \quad & P_s|\hat{h}_p+e_p|^2 \leq q, \\ & P_s \leq P_t, P_s \geq 0. \end{aligned} \tag{15}$$

First, we introduce the Charnes-Cooper transformation [42] as

$$\overline{P}_s = \frac{P_s}{t}, \tag{16}$$

to recast the problem defined in (15) as

$$\begin{aligned} \max_{\overline{P}_s,\ t} \quad & t + \frac{\overline{P}_s|\hat{h}_s+e_s|^2}{P_p|g_s|^2+\sigma_s^2} \\ s.t. \quad & t + \frac{\overline{P}_s|\hat{h}_e+e_e|^2}{P_p|g_e|^2+\sigma_e^2} \leq 1, \\ & \overline{P}_s|\hat{h}_p+e_p|^2 \leq tq, \\ & \overline{P}_s \leq tP_t, \overline{P}_s \geq 0. \end{aligned} \tag{17}$$

The problem defined in (17) can be rewritten by introducing a new slack variable τ and defining it in the epigraph form as

$$\max_{\overline{P}_s,\ t,\ \tau} \quad \tau \tag{18a}$$

$$s.t. \quad t + \frac{\overline{P}_s|\hat{h}_s+e_s|^2}{P_p|g_s|^2+\sigma_s^2} \geq \tau, \tag{18b}$$

$$t + \frac{\overline{P}_s|\hat{h}_e+e_e|^2}{P_p|g_e|^2+\sigma_e^2} \leq 1, \tag{18c}$$

$$\overline{P}_s|\hat{h}_p+e_p|^2 \leq tq, \tag{18d}$$

$$\overline{P}_s \leq tP_t, \overline{P}_s \geq 0. \tag{18e}$$

The above problem is still intractable due to the infinite number of the uncertainty sets in the constraints (18b)-(18d). To address this issue, we employ the following proposition:

Proposition 1: : The constraints in (18b)-(18d) can be equivalently written as

$$\begin{aligned} & \begin{bmatrix} \lambda_1 + \frac{\overline{P}_s}{P_p|g_s|^2+\sigma_s^2} & \frac{\overline{P}_s\hat{h}_s}{P_p|g_s|^2+\sigma_s^2} \\ \frac{\overline{P}_s\hat{h}_s}{P_p|g_s|^2+\sigma_s^2} & \frac{\overline{P}_s|\hat{h}_s|^2}{P_p|g_s|^2+\sigma_s^2} + t - \tau - \lambda_1\epsilon_s^2 \end{bmatrix} \succeq \mathbf{0}, \\ & \lambda_1 \geq 0, \end{aligned} \tag{19}$$

$$\begin{aligned} & \begin{bmatrix} \lambda_2 - \frac{\overline{P}_s}{P_p|g_e|^2+\sigma_s^2} & -\frac{\overline{P}_s\hat{h}_e}{P_p|g_e|^2+\sigma_s^2} \\ -\frac{\overline{P}_s\hat{h}_e}{P_p|g_e|^2+\sigma_s^2} & 1 - \frac{\overline{P}_s|\hat{h}_s|^2}{P_p|g_e|^2+\sigma_e^2} - t - \lambda_2\epsilon_e^2 \end{bmatrix} \succeq \mathbf{0}, \\ & \lambda_2 \geq 0, \end{aligned} \tag{20}$$

and

$$\begin{aligned} & \begin{bmatrix} \lambda_3 - \overline{P}_s & -\overline{P}_s\hat{h}_p \\ -\overline{P}_s\hat{h}_p & tq - \overline{P}_s|\hat{h}_p|^2 + \sigma_s^2 - \lambda_e\epsilon_p^2 \end{bmatrix} \succeq \mathbf{0}, \\ & \lambda_3 \geq 0. \end{aligned} \tag{21}$$

Proof: Please refer to Appendix A. ■

Therefore, we rewrite the problem in (18) into the following equivalent form:

$$\begin{aligned} \max_{\overline{P}_s,\ t,\ \tau} \quad & \tau \\ s.t. \quad & \text{(19)-(21)}, \\ & \overline{P}_s \leq tP_t, \overline{P}_s \geq 0. \end{aligned} \tag{22}$$

The above problem is convex, and therefore, the optimal P_s^* can be obtained efficiently by the convex optimization tool box [48].

IV. Power Allocation Framework based on NN

In this section, we present our proposed NN-based schemes. In this approach, the secrecy rate maximization problem is treated as an unknown non-linear mapping, and an NN is trained to learn the relationship between the input and the output parameters.

First, NNs can be considered as universal function approximators [49] and shown to have remarkable capabilities of algorithmic learning [50]. As such, they are akin to conventional optimizer-based solutions. Second, the literature demonstrate that NN schemes have the capability to substantially reduce the computational complexity, and processing time for a variety of problems in wireless communications, such as, resource allocation [33], [35], [51], channel estimation and signal detection [30], and physical layer designs [39]. Third, once the networks are trained (ideally using scalable computational resources), the resulting model is suitable for inference in very limited resource for real-time applications [52].

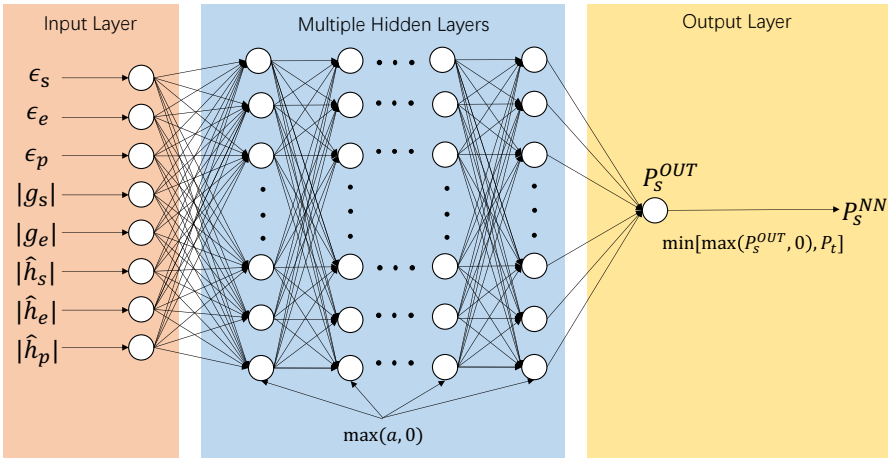

Fig. 2: The structure of proposed NN.

Remark 1: Although the notion of function approximation is useful to derive a powerful learned model, rendering an adaptive learning model is a challenging goal, including, but not limited to, anticipating varying inputs, noisy conditions, and failures. As such, a simple NN-based approach alone cannot handle dynamic problems effectively. Instead, a solution to a dynamic problem will involve a hybrid approach, covering optimization techniques, NN, on-line learning, reinforcement learning and possibly other techniques.

Remark 2: The proposed NN-based approach performs its derivations in real domain to determine the weights and bias through minimizing loss functions. However, a problem might arise that the complex derivations exist if and only if the loss functions satisfy the Cauchy-Riemann equations. In the complex domain, the functions that satisfy these equations are called holomorphic functions; otherwise, they are called non-holomorphic functions [53]. This condition for complex domain introduces challenges for directly employing the proposed NN-based approach to learn to optimize in multiple antenna wireless communication systems. For example, in holographic multiple-input multiple-output (MIMO) surfaces and reconfigurable intelligent surfaces aided future wireless networks, the NNs need to deal with different parameters in complex domains.

Our aim is to utilize the high computational efficiency of the NN in its testing stage to design a time and computational efficient real-time power allocation scheme which can be applied to solve the power allocation problem with both perfect and imperfect CSI. As shown in Fig. 2, the proposed NN consists of three layers: input layer, multiple hidden layers and output layer. In particular, we choose $|\hat{h}_s|$, $|\hat{h}_p|$, $|\hat{h}_e|$, $|g_s|$, $|g_e|$, ϵ_s, ϵ_e and ϵ_p as inputs and P_s^* as output of the training data, respectively. Note that the perfect CSI scheme becomes a special case of imperfect CSI scheme by setting the inputs for the perfect CSI scheme as $|\hat{h}_s| = |h_s|$, $|\hat{h}_p| = |h_p|$, $|\hat{h}_e| = |h_e|$, and $\epsilon_s = \epsilon_e = \epsilon_p = 0$. The mapping between the input and the output parameters can be expressed as

$$P_s^* = f(|\hat{h}_s|, |\hat{h}_p|, |\hat{h}_e|, |g_s|, |g_e|, \epsilon_s, \epsilon_e, \epsilon_p). \tag{23}$$

We start from the input and then pass the input data through the NN and calculate the actual output straightforwardly, which is referred as feed-forward. Furthermore, the calculation flow follows the natural forward direction from the input layer to the hidden layers and finally to the output layer. This process can be expressed mathematically as

$$\mathbf{z}^{(l+1)} = \mathbf{W}^{(l)}\mathbf{a}^{(l)} + \mathbf{b}^{(l)}, \tag{24}$$

$$\mathbf{a}^{(l+1)} = g(\mathbf{z}^{(l+1)}), \tag{25}$$

where $\mathbf{z}^{(l+1)}$ is the linear transformation of given inputs at the $(l+1)$-th layer, whereas $\mathbf{a}^{(l+1)}$ is the output activation value of the $(l+1)$-th layer. $g(\mathbf{z})$ denotes the activation function; in this work, we choose the rectified linear unit (ReLU) function as the activation function, which can be expressed as $g(x) = \max\{0, x\}$. $\mathbf{W}^{(l)}$ and $\mathbf{b}^{(l)}$ are the weight matrix and the bias vector for the l-th layer, respectively. Suppose there is an N-layer NN, the mapping between the inputs and the output parameters can be expressed as

$$y = f(\mathbf{S}, \mathbf{W}, \mathbf{b}), \tag{26}$$

where $\mathbf{S} = [|\hat{h}_s|, |\hat{h}_p|, |\hat{h}_e|, |g_s|, |g_e|, \epsilon_s, \epsilon_e, \epsilon_p]$. Our goal is to determine the weights $\mathbf{W} = [\mathbf{W}^{(1)}, ..., \mathbf{W}^{(N-1)}]$ and the bias $\mathbf{b} = [\mathbf{b}^{(1)}, ..., \mathbf{b}^{(N-1)}])$ such that both functions in (23) and (26) yield a similar output for the same set of inputs.

Proposition 2: In order to have a similar outputs from both (23) and (26), we should minimize the following normalized loss function:

$$J(\mathbf{W}, \mathbf{b}) = \frac{1}{M}\sum_{m=1}^{M}(y_m - P_{s,m}^*)^2, \tag{27}$$

where M is the number of training data sets. y_m and $P^*_{s,m}$ are the m-th output of the NN and the optimal transmit power obtained by the conventional optimization approach, respectively.

Proof: Please refer to Appendix B. ■

We iteratively use the back-propagation based gradient descent algorithm to update the weights matrices $\mathbf{W}$ and the bias vectors $\mathbf{b}$.

Proposition 3: Based on the back-propagation and the gradient descent algorithm, the weight matrix and the bias vector for the l-th layer $\mathbf{W}^{(l)}$ and $\mathbf{b}^{(l)}$ can be updated respectively by

$$\mathbf{W}^{(l)} = \mathbf{W}^{(l)} - \frac{\alpha}{M}\sum_{m=1}^{M}[\boldsymbol{\delta}_m^{(l+1)}(\mathbf{a}_m^{(l)})^T], \tag{28}$$

$$\mathbf{b}^{(l)} = \mathbf{b}^{(l)} - \frac{\alpha}{M}\sum_{m=1}^{M}\boldsymbol{\delta}_m^{(l+1)}, \tag{29}$$

where α is the learning rate and $\boldsymbol{\delta}_m^{(l+1)}$ is defined as $\boldsymbol{\delta}_m^{(l+1)} = \frac{\partial J(\mathbf{W},\mathbf{b})}{\partial \mathbf{z}_m^{(l+1)}}$.

Proof: Please refer to Appendix C. ■

In an NN, over-fitting is the result of a model that is very closely to or precisely aligned to a specific set of data [54], which occurs when the model learns the training data set along with noises [55]. Over-fitting leads the model not to be able to fit additional data or reliably predict future observations [54]. Regularization is an approach to reduce the well-known over-fitting problem of a machine learning model [56], [57]. To overcome this over-fitting problem, the L_1 and L_2 regularizations are most widely utilized techniques in the literature [58], [59].

The regularization term is added to the loss function to reduce the sum of absolute values of the weights in the L_1 regularization method, where the loss function can be written as

$$J(\mathbf{W},\mathbf{b}) = \frac{1}{M}\sum_{m=1}^{M}(y_m - P^*_{s,m})^2 + \frac{\lambda}{2M}\sum_{l=1}^{N-1}||\mathbf{W}^{(l)}||_1, \tag{30}$$

where λ is the regularization parameter. Following the similar derivation of Proposition 2, the weights for the L_1 regularization can be updated as

$$\mathbf{W}^{(l)} = -\frac{\alpha}{M}\sum_{m=1}^{M}[\boldsymbol{\delta}_m^{(l+1)}(\mathbf{a}_m^{(l)})^T] - \frac{\alpha\lambda}{M}. \tag{31}$$

The bias $\mathbf{b}^{(l)}$ can be updated by using the equation provided in (29).

In the L_2 regularization method, the sum of squares of the weights are reduced by adding the regularization term to the loss function, which can be mathematically expressed as

$$J(\mathbf{W},\mathbf{b}) = \frac{1}{M}\sum_{m=1}^{M}(y_m - P^*_{s,m})^2 + \frac{\lambda}{2M}\sum_{l=1}^{N-1}||\mathbf{W}^{(l)}||_2^2, \tag{32}$$

where λ is the regularization parameter. Following a derivation similar to that of Proposition 2, the weights for the L_2 regularization can be updated as

$$\mathbf{W}^{(l)} = (1 - \frac{\alpha\lambda}{M})\mathbf{W}^{(l)} - \frac{\alpha}{M}\sum_{m=1}^{M}[\boldsymbol{\delta}_m^{(l+1)}(\mathbf{a}_m^{(l)})^T]. \tag{33}$$

The bias $\mathbf{b}^{(l)}$ for L_2 regularization can be updated by using the equation provided in (29).

The development of our proposed NN scheme can be divided into three steps: (1) Obtaining the training data set by solving the secrecy rate maximization problem through conventional optimization approach; (2) developing an NN-based algorithm to learn the relationship between the input and output parameters of this secure transmission system; (3) after completing the training process, evaluating the performance of the trained NN over the conventional optimization algorithm. The details of these steps are provided in Algorithm 2.

V. Simulation Results

In this section, we present numerical results to demonstrate the superior performance of our proposed NN schemes. The data set is obtained by utilizing the conventional optimization scheme in Section III with 6×10^5 different random channel realizations. We split the data set into two subsets of data: 5×10^5 for training and 10^5 for validation. In the training process, all the NN parameters are updated by utilizing mini-batch gradient descent algorithm based on the Adam optimizer [60], where the batch size is chosen to be ten. All the parameters in NN are initialized with by the Xavier initializer [61]. Furthermore, similar to [33], it is assumed that the NN has two hidden layers with one hundred neurons in each layer. The learning rate α is set to 10^{-4} and the regularization parameter λ is assumed to be 5×10^{-4} [28], [58], [62]. The test data set is obtained by using 3000 channel realizations. The transmit power of PU-Tx is assumed to be 60 mW, whereas all the noise variances are set to be 0.001. The channels $\hat{h}_s, \hat{h}_p, \hat{h}_e, g_s$, and g_e are all generated by $\hat{h}_i = \chi_i\sqrt{d_i^{-\alpha}}$, $i = s, e, p$ and $g_j = \chi_j\sqrt{c_j^{-\alpha}}$, $j = s, e$, where $\chi_i \sim \mathcal{CN}(0,1)$, $\chi_j \sim \mathcal{CN}(0,1)$, d_i is the distance between the SU-Tx and the i-th user and c_j denotes the distance between the PU-Tx and the i-th user. The parameter $\alpha = 1.7$ denotes the path loss exponent. The distances between the transmitters and corresponding receivers are assumed to be $d_s = 10$ m, $d_e = 20$ m, $d_p = 10$ m, $c_s = 20$ m and $c_e = 20$ m, respectively. The simulated datasets for training and testing were generated using MATLAB scripts, and the performance of data generation is irrelevant to the results. For training and testing the model, we used a system with Intel Core i7-9700K

Algorithm 2: The NN approach

Preparing process:

1: Obtain the training data set by utilizing the conventional approaches in Section III: The optimal transmit power P_s^* for corresponding the channel coefficients $|\hat{h}_s|, |\hat{h}_p|, |\hat{h}_e|, |g_s|, |g_e|$ and channel error bounds $\epsilon_s, \epsilon_e, \epsilon_p$;

Training process:

1: Initialize the weights matrices $\mathbf{W}$, the bias vectors $\mathbf{b}$ and the learning rate α;
2: Divide the training data set into I mini-batches, the size of each mini-batch is M;
3: **For each batch**: Input the training set $\mathbf{S} = [\mathbf{S}_1, \ldots, \mathbf{S}_M]$ and $\mathbf{y} = [y_1, \ldots, y_M]$, where $\mathbf{S}_m = [|\hat{h}_{s,m}|, |\hat{h}_{p,m}|, |\hat{h}_{e,m}|, |g_{s,m}|, |g_{e,m}|, \epsilon_{s,m}, \epsilon_{e,m}, \epsilon_{p,m}]$;
4: For NN without any regularization, update the weights matrices $\mathbf{W}$ and the bias vectors $\mathbf{b}$ by minimizing the loss function defined in (27) using the back-propagation based gradient descent method provided in (28) and (29);
5: For NN with L_1 regularization, update the weights matrices $\mathbf{W}$ and the bias vectors $\mathbf{b}$ by utilizing the back-propagation based gradient descent method provided in (31) and (29), which are based on minimizing the loss function defined in (30);
6: For NN with L_2 regularization, update the weights matrices $\mathbf{W}$ and the bias vectors $\mathbf{b}$ by minimizing the loss function defined in (32) using the back-propagation based gradient descent method provided in (33) and (29);
7: **End for**;
8: Save the trained NN.

Testing process:

1: Generate the channel coefficients for the test data set $\mathbf{S}_{test}$:
2: Feed $\mathbf{S}_{test}$ as the input parameters and determine the output results based on the trained NN;

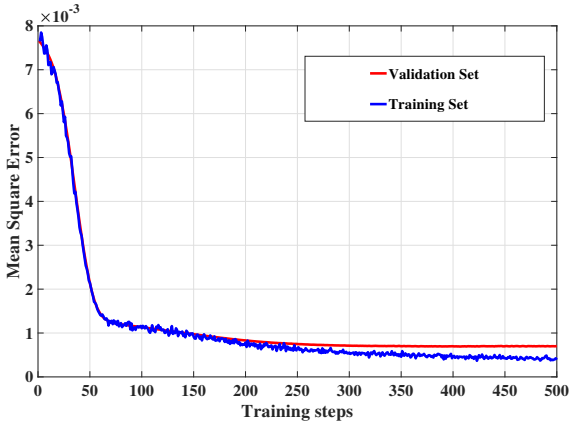

Fig. 3: The mean square error between the power allocations obtained by the conventional approach and the NN scheme without regularization versus the number of training steps.

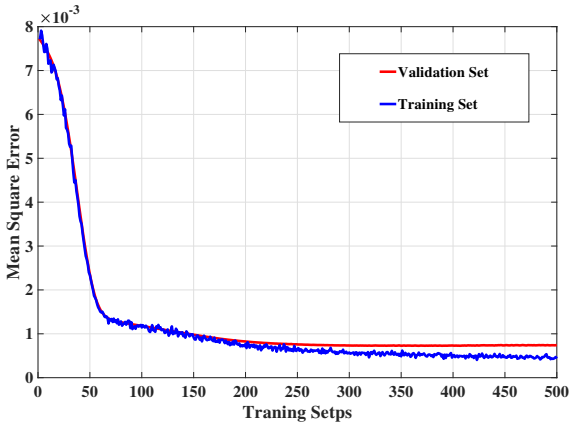

Fig. 4: The mean square error between the power allocations obtained by the conventional approach and the NN scheme with L_1 regularization versus the number of training steps.

processor, with eight cores, clocked at 3.9 GHz, 12 MB cache memory and 32 GB random access memory. The training was performed purely on CPUs (opposed to GPUs).

First, we show the mean square error obtained by NN schemes without regularization, with L_1 regularization and L_2 regularization versus the number of training steps, respectively, in Figs. 3-5. For a better presentation, we take samples for every 100 points from the whole training steps. It is obvious that the mean square error decreases and approaches zero as the number of iterations increases. This is due to the fact that the weights $\mathbf{W}$ and the bias $\mathbf{b}$ of the NN are iteratively updated by using the mini-batch gradient descent algorithm. Furthermore, the mean square errors of the validation data for the three schemes are also provided, respectively, in Figs. 3-5. As seen in these figures, the mean square errors first decrease and then remain constant, which confirms that the training process does not over-fit the NN for all three cases. Over-fitting is a phenomenon where a machine learning model becomes overly sensitive to a given dataset, and hence, fails to generalize beyond the training data [9], [28], [63]. Generally, a model can easily be tested for over-fitting using a validation dataset that the model has not been exposed to. An over-fitted model has a signature characteristic of performing well for few training steps, and showing degrading performance for larger training steps [9], [28], [63], while the training performance increases. In our cases, it can be seen that the validation performance approaches a stead-state with increasing training steps. This is a clear evidence that the model is not over-fitted.

Next, Fig. 6 presents the performance comparison in terms of optimal transmit power obtained by using the conventional optimization scheme and the proposed NN scheme (without regularization) versus the number of training steps. Similar to Figs. 3-5, the results of this figure are obtained by sampling every 100 points from the whole training steps. As seen in this figure, the output transmit power of the proposed NN scheme approaches the optimal transmit power obtained from the conventional scheme as the training steps increase. The reason is that the weights $\mathbf{W}$ and the bias $\mathbf{b}$ of the proposed NN are continuously updated in the training process to achieve minimum mean square error. Note that the output power of the proposed NN may be negative or larger than the available transmit power, since the training errors between the NN

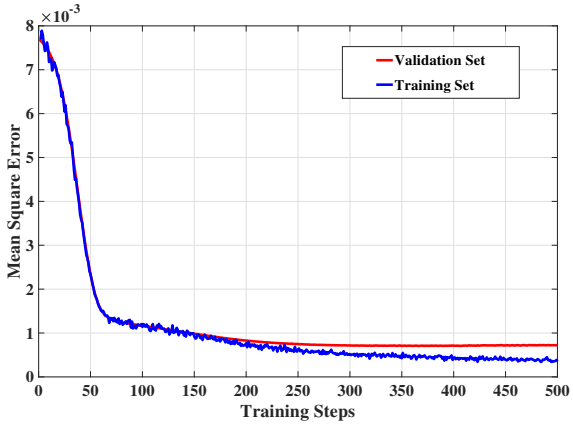

Fig. 5: The mean square error between the power allocations obtained by the conventional approach and the NN scheme with L_2 regularization versus the number of training steps.

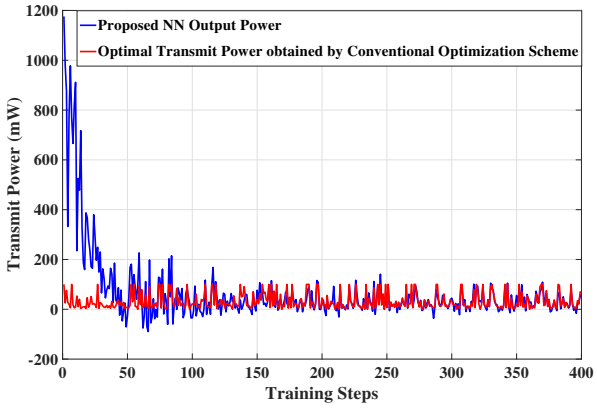

Fig. 6: The performance comparison in terms of the optimal transmit power obtained by the conventional optimization approach and the proposed NN-based scheme without regularization versus the number of training steps.

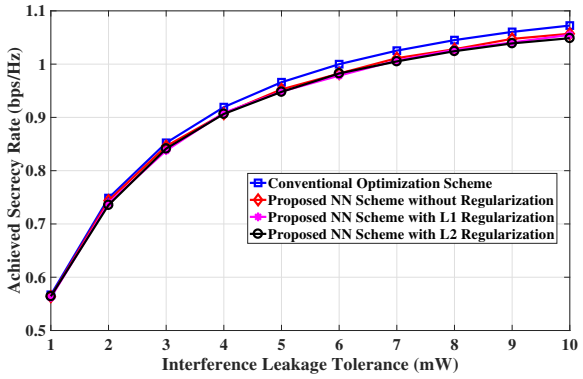

Fig. 7: The achievable secrecy rates versus the interference tolerance of the PU-Rx obtained by the conventional optimization approach and the proposed NN framework under perfect CSI assumption.

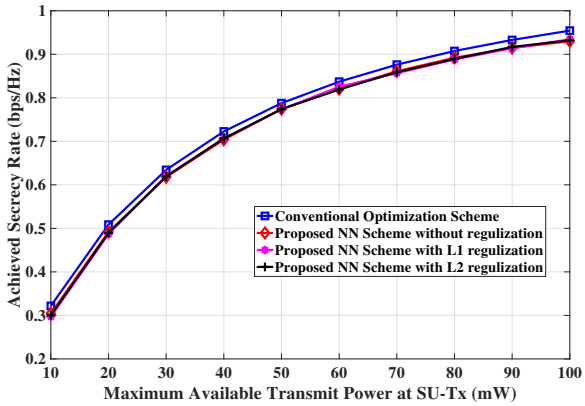

Fig. 8: The achievable secrecy rates versus the maximum transmit power of the SU-Tx obtained by the conventional optimization approach and the proposed NN framework under perfect CSI assumption.

output power and the optimal power obtained by conventional optimization scheme cannot be completely eliminated. In order to incorporate the power constraints ($0 \leq P_s \leq P_t$), we choose $P_s^{NN} = \min(\max(P_s^{OUT}, 0), P_t)$ as the SU-Tx transmit power of our proposed NN scheme in the following simulation results.

Next, Fig. 7 presents the achievable secrecy rates of the SU-Rx versus the interference leakage tolerance of the PU-Rx obtained by both conventional optimization and our proposed NN schemes with perfect CSI assumption. The maximum available transmit power of the SU-Tx is assumed to be 100 mW. It can be seen that the achievable secrecy rate increases with the interference leakage tolerance for all schemes. In addition, the three NN-based schemes can achieve a similar performance with the conventional optimization approach. Note that there is a performance gap between the conventional scheme and the three NN schemes, and this is due to the training errors between the output power and the desired optimal power.

Next, we evaluate the achievable secrecy rates versus the available transmit power with perfect CSI. Fig. 8 presents the achievable secrecy rates of SU-Rx of both conventional optimization and our proposed NN schemes. The interference leakage tolerance is set to 6 mW. It can be seen that the achievable secrecy rate increases as the transmit power enhances for all schemes. Similar to Fig. 7, our proposed NN schemes show a similar performance as the conventional optimization approach.

Next, Fig. 9 presents the achievable secrecy rates versus the interference leakage tolerance at the PU-Rx obtained by both conventional optimization and our proposed NN schemes under imperfect CSI assumption. The channel error bound is assumed to be $\epsilon_s = \epsilon_e = \epsilon_p = 0.1$. The maximum available transmit power of SU-Tx is assumed to be 100 mW. As seen in Fig. 9, the achievable secrecy rate enhances as the interference leakage tolerance increases for all schemes. Furthermore, the three NN-based schemes show similar performances compared to that of the conventional optimization approach.

Next, we evaluate the achievable secrecy rates of conventional optimization and the proposed NN schemes with different available transmit power at SU-Tx. Fig. 10 presents the achievable secrecy rates of SU-Rx for these schemes. The interference leakage tolerance is set to 6 mW. As seen in Fig.

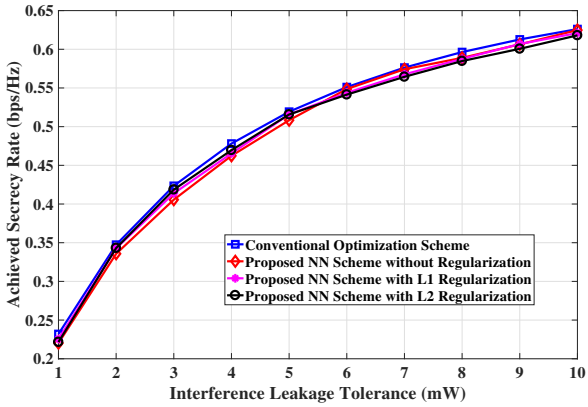

Fig. 9: The achievable secrecy rates versus the interference tolerance of the PU-Rx obtained by the conventional optimization approach and the proposed NN framework under imperfect CSI assumption.

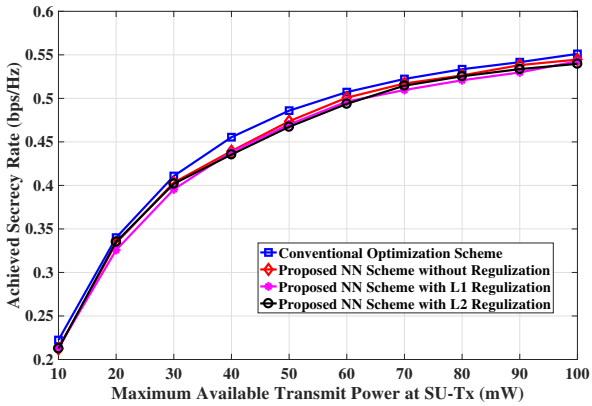

Fig. 10: The achievable secrecy rates versus the maximum transmit power of the SU-Tx obtained by the conventional optimization approach and the proposed NN framework under imperfect CSI assumption.

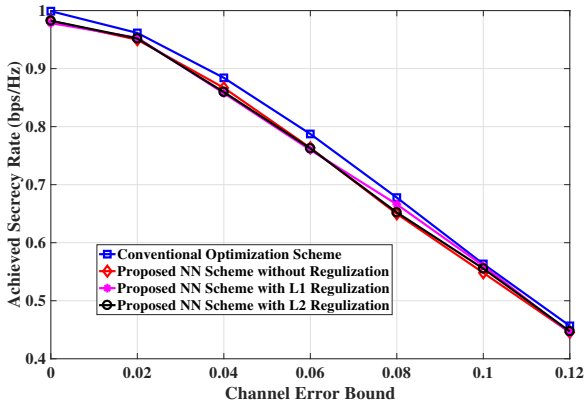

Fig. 11: The achievable secrecy rates versus channel error bounds obtained by the conventional optimization approach and the proposed NN framework.

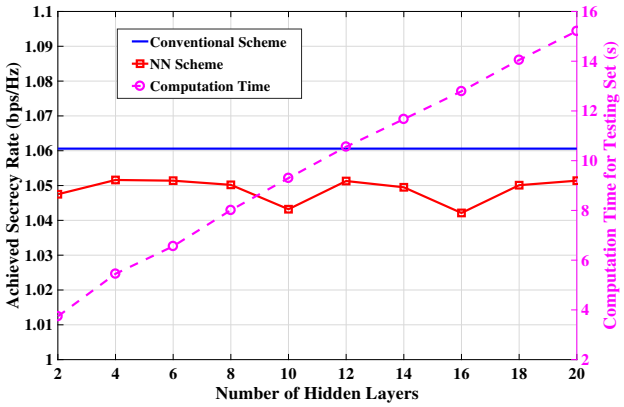

Fig. 12: The achievable secrecy rates (left axis) and computation time for the training set (right axis) versus the number of hidden layers.

10, the achievable secrecy rate enhances with the increase in the interference leakage tolerance. Similar to previous results, the proposed NN schemes provide a similar performance as the conventional convex optimization approach.

The achievable secrecy rates of conventional optimization and proposed NN schemes with different channel error bounds are provided in Fig. 11. The maximum available transmit power at SU-Tx is set to be 100 mW and the interference leakage tolerance at PU-Rx is assumed to be 6 mW. All the channel error bounds are assumed to be the same for each point, i.e., $\epsilon_s = \epsilon_e = \epsilon_p$. As seen in this figure, the achieved secrecy rate decreases as the channel error bound increases for all the schemes. Furthermore, as observed in the previous set of simulation results, the proposed NN schemes can achieve similar performances in comparison with the conventional convex optimization scheme.

In Fig. 12, we present the achieved secrecy rate (left axis) and computation time (right axis) versus the number of hidden layers for the NN scheme without any regularization. The maximum available transmit power at the SU-Tx and the interference leakage tolerance at the PU-Rx are assumed to be 100 mW and 9 mW, respectively. All channel error bounds are set to be 0 to represent the perfect CSI scenario. As shown in this figure, the difference of performance among different number of hidden layers are within a range of 1%. However, the computation time for the testing set increases as the number of hidden layers increase. In other words, introducing more hidden layers cannot lead to much performance improvement, while it will yield more computational complexity to the NN.

Next, we present the statistical results in Figs. 13 and 14 to evaluate the interference leakage tolerance satisfaction at the PU-Rx for the proposed NN scheme without regularization. These statistical results are calculated by combing the results of test data of both perfect and imperfect CSI scenarios. In Fig. 13, the interference leakage tolerance is set to 6 mW, while the maximum available transmit power at the SU-Tx is assumed to be 100 mW in Fig. 14. Fig. 13 provides the interference leakage tolerance satisfaction versus the maximum transmit power, whereas Fig. 14 presents it versus the interference leakage tolerances. As shown in these figures, more than 93% of the test results can meet the interference leakage constraint at the PU-Rx.

Table I provides the secrecy rate performance of all schemes with perfect and imperfect CSI versus different interference

TABLE I: The achieved secrecy rates of all schemes versus the interference leakage tolerances

Perfect CSI

Interference leakage tolerance (mW)	NN scheme without regularization (bps/Hz)	NN scheme with L_1 regularization (bps/Hz)	NN scheme with L_2 regularization (bps/Hz)	Conventional scheme (bps/Hz)	Minimum ratio (%)
1	0.5636	0.5618	0.5642	0.5679	98.93
2	0.7438	0.7393	0.7355	0.7486	98.25
3	0.846	0.8377	0.8414	0.8523	98.29

Imperfect CSI

Interference leakage tolerance (mW)	NN scheme without regularization (bps/Hz)	NN scheme with L_1 regularization (bps/Hz)	NN scheme with L_2 regularization (bps/Hz)	Conventional scheme (bps/Hz)	Minimum ratio (%)
1	0.2202	0.2256	0.2216	0.2320	94.91
2	0.3357	0.3427	0.3431	0.3474	96.63
3	0.4056	0.4138	0.4186	0.4235	95.77

TABLE II: The required computational time for all schemes versus the interference leakage tolerances

Perfect CSI

Interference leakage tolerance (mW)	NN scheme without regularization (s)	NN scheme with L_1 regularization (s)	NN scheme with L_2 regularization (s)	Conventional scheme (s)	Maximum ratio (%)
1	3.59	4.40	4.38	558.71	0.79
2	3.69	4.58	4.47	584.68	0.78
3	3.77	4.45	4.46	573.38	0.78

Imperfect CSI

Interference leakage tolerance (mW)	NN scheme without regularization (s)	NN scheme with L_1 regularization (s)	NN scheme with L_2 regularization (s)	Conventional scheme (s)	Maximum ratio (%)
1	3.72	4.67	4.22	651.18	0.65
2	3.71	4.79	4.39	639.32	0.75
3	3.62	4.74	4.29	647.28	0.73

TABLE III: The achieved secrecy rates of all schemes versus the maximum transmit powers

Perfect CSI

Maximum available transmit power (mW)	NN scheme without regularization (bps/Hz)	NN scheme with L_1 regularization (bps/Hz)	NN scheme with L_2 regularization (bps/Hz)	Conventional scheme (bps/Hz)	Minimum ratio (%)
10	0.5636	0.5618	0.5642	0.5679	98.93
20	0.7438	0.7393	0.7355	0.7486	98.25
30	0.846	0.8377	0.8414	0.8523	98.29

Imperfect CSI

Maximum available transmit power (mW)	NN scheme without regularization (bps/Hz)	NN scheme with L_1 regularization (bps/Hz)	NN scheme with L_2 regularization (bps/Hz)	Conventional scheme (bps/Hz)	Minimum ratio (%)
10	0.2123	0.2138	0.2127	0.2224	95.46
20	0.3338	0.3258	0.3351	0.3400	95.82
30	0.4033	0.3954	0.4019	0.4108	96.25

TABLE IV: The required computational time for all schemes versus the maximum transmit powers

Perfect CSI

Maximum available transmit power (mW)	NN scheme without regularization (s)	NN scheme with L_1 regularization (s	NN scheme with L_2 regularization (s)	Conventional scheme (s)	Minimum ratio (%)
10	4.21	5.03	5.34	578.06	0.92
20	3.90	4.65	4.77	574.38	0.83
30	3.63	4.39	4.58	566.87	0.81

Imperfect CSI

Maximum available transmit power (mW)	NN scheme without regularization (s)	NN scheme with L_1 regularization (s)	NN scheme with L_2 regularization (s)	Conventional scheme (s)	Minimum ratio (%)
10	3.87	4.62	4.76	658.36	0.72
20	4.07	4.52	4.44	654.87	0.69
30	3.93	4.82	4.68	661.43	0.73

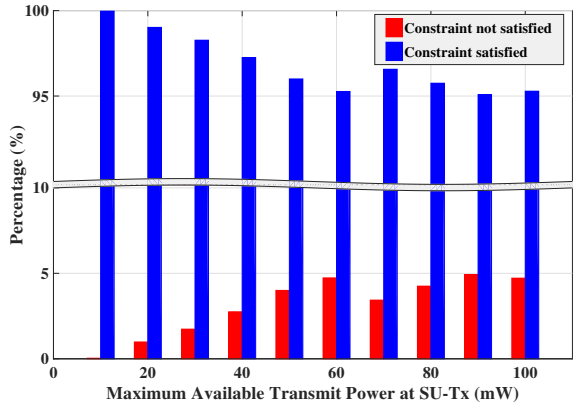

Fig. 13: Distributions of the interference leakage satisfactions versus the maximum available transmit power at SU-Tx.

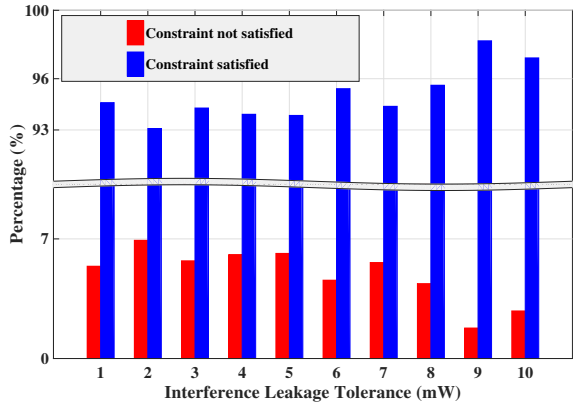

Fig. 14: Distributions of the interference leakage satisfactions versus the interference leakages at RU-Rx.

leakage tolerances, similar to the results depicted in Figs. 7 and 9. Table II shows the comparison of the required computation time of the four schemes versus the interference leakage tolerances. Similarly, Table III presents the achieved the secrecy rate performance of all schemes versus the available transmit power. Table IV provides the required computation time of all schemes versus the maximum transmit power. To draw a performance comparison of the achieved secrecy rate, we employ the minimum ratio, which is calculated by dividing the minimum achieved secrecy rate among the three NN schemes by that of the conventional scheme. Similarly, for the comparison of the computational time, we use the maximum ratio, which is obtained by dividing the maximum computation of the three NN schemes by that of the conventional scheme. Note that the testing process for all schemes is performed on the same computer. For the results provided in these tables, the achievable secrecy rates are obtained by averaging results over the test data with 3000 channel realizations, while the computational time is the total computation time of 3000 channel realizations. From these results, we can conclude that the proposed NN schemes achieve at least 94% of the optimal performance of the conventional scheme, while significantly reducing the required computation time. In particular, the proposed NN-based schemes require less than 1% of the time needed by the conventional optimization scheme. This is due to the fact that the conventional optimization based solutions of the perfect CSI assumption are obtained through an iterative approach and sub-gradient algorithms, while the conventional scheme for the imperfect CSI assumption requires sub-gradient algorithms. These conventional optimization algorithms for both perfect and imperfect CSI scenarios are more complexity, which require a higher computation time. In the NN-based schemes, once the weights and bias are determined, it is should be able to compute the solution with a reasonable complexity within a short time compared to that of the conventional approach.

VI. Discussions

Despite offering a number of benefits, the proposed approach also has a number of shortcomings. We discuss these below, and highlight a number of potential directions for future work:

1) NN is a supervised learning approach, and hence relies on labelled-data for training the NN. In our context, the the necessity for valid labels implies that the training data should also be reliable, which is required for guaranteeing a valid solution [9]. In addition, the training is an off-line process, which effectively limits the applicability of the proposed approach to dynamic wireless systems. As we have mentioned in *Remark 1*, hybrid approaches can be considered for problems in dynamic systems, which might include optimization techniques, NN, on-line learning, reinforcement learning and possibly other techniques.
2) As mentioned in *Remark 2*, the proposed NN approach may not be able to learn to optimize for multiple-antenna wireless transmission scenarios. To extend this NN-based scheme to multiple-antenna systems, one can consider two approaches. One is to is to separate both complex input and output parameters into real and imaginary parts [64], and the NN can be trained in real domain. The other is to handle the complex parameters by employing the Wirtinger calculus to deal with non-holomorphic functions in complex domain [53].
3) Finally, due to the fact that training errors cannot be completely eliminated, the proposed NN cannot include constraints in the training process, as presented in Fig. 13 and Fig. 14. This introduces challenges for extending the proposed scheme to design problems that have numerous system constraints. Fortunately, a constrained training algorithm was developed in the literature [65], where the key idea is to employ the Lagrange dual formulation to accommodate the constraints [48]. This is another potential direction of future research work.

VII. Conclusion

In this paper, we proposed an NN-based approach for the power allocation design to maximize the secrecy rate in a CR network under transmit power and interference leakage constraints. We showed that the developed NN algorithm has

the capability to solve the power allocation problem with both perfect and imperfect CSI, whereas it requires to develop both robust and non-robust optimization frameworks in the conventional approach. First, the conventional optimization scheme for perfect CSI scenario was developed based on a one-dimensional search, while that for the imperfect assumption was developed based on the Charnes-Cooper transformation and the S-Procedure approach. Then, the NN-based schemes were proposed where a relationship between the input and output parameters is established by determining an approximated function. The training set to determine the relationship between inputs and output was obtained through the conventional optimization approaches and the NN was trained to calculate the weights of the connections in the network. After training the NN, the performance was evaluated with a test set in terms of achieved secrecy rate and required computational time. We demonstrated that the proposed NN schemes can achieve more than 94% of the secrecy rate performance with less than 1% computation time and more than 93% satisfaction of interference leakage constraints compared with those of the conventional approaches. Simulation results were provided to demonstrate the effectiveness of the proposed NN-based approach over the benchmark conventional optimization approaches. Finally, we have discussed some limitations of the proposed NN-based approach and a number of potential future directions of research.

Appendix A
Proof of Proposition 1

First, we consider the following Lemma:

Lemma 1: (*S-Procedure* [43]) Define $f_i(\mathbf{x})$, $i = 1, 2$ such as

$$f_i(\mathbf{x}) = \mathbf{x}^H \mathbf{A}_i \mathbf{x} + 2Re\{\mathbf{b}_i^H \mathbf{x}\} + c_i, \tag{34}$$

in which $\mathbf{x} \in \mathcal{R}^n$, $\mathbf{A}_i \in \mathcal{S}^n$, $\mathbf{b}_i \in \mathcal{R}^n$ and $c_i \in \mathcal{R}$. The implication $f_1(\mathbf{x}) \leq 0 \rightarrow f_2(\mathbf{x}) \leq 0$ holds if and only if there exists a $\vartheta \geq 0$ such that

$$\vartheta \begin{bmatrix} \mathbf{A}_1 & \mathbf{b}_1 \\ \mathbf{b}_1^H & c_1 \end{bmatrix} - \begin{bmatrix} \mathbf{A}_2 & \mathbf{b}_2 \\ \mathbf{b}_2^H & c_2 \end{bmatrix} \succeq \mathbf{0}. \tag{35}$$

We first rewrite the constraint in (18b) as

$$\begin{aligned} &|e_s|^2 - \epsilon_s^2 \leq 0, \\ &\tau - t - \frac{\overline{P}_s |\hat{h}_s|^2 + 2Re\{\overline{P}_s \hat{h}_s e_e\}}{+} \overline{P}_s |e_s|^2 P_p |g_s|^2 + \sigma_s^2 \leq 0. \end{aligned} \tag{36}$$

Then, by applying Lemma 1, this constraint can be reformulated with a slack variable λ_1 as

$$\begin{aligned} &\begin{bmatrix} \lambda_1 + \frac{\overline{P}_s}{P_p |g_s|^2 + \sigma_s^2} & \frac{\overline{P}_s \hat{h}_s}{P_p |g_s|^2 + \sigma_s^2} \\ \frac{\overline{P}_s \hat{h}_s}{P_p |g_s|^2 + \sigma_s^2} & \frac{\overline{P}_s |\hat{h}_s|^2}{P_p |g_s|^2 + \sigma_s^2} + t - \tau - \lambda_1 \epsilon_s^2 \end{bmatrix} \succeq \mathbf{0}, \\ &\lambda_1 \geq 0. \end{aligned} \tag{37}$$

Similarly, (18c) and (18d) also can be derived as

$$\begin{aligned} &|e_e|^2 - \epsilon_e^2 \leq 0, \\ &t - 1 + \frac{\overline{P}_s |\hat{h}_e|^2 + 2Re\{\overline{P}_s \hat{h}_e e_e\} + \overline{P}_s |e_e|^2}{P_p |g_e|^2 + \sigma_e^2} \leq 0, \end{aligned} \tag{38}$$

and

$$\begin{aligned} &|e_e|^2 - \epsilon_e^2 \leq 0, \\ &\overline{P}_s |\hat{h}_p|^2 + 2Re\{\overline{P}_s \hat{h}_p e_p\} + \overline{P}_s |e_p|^2 - tq \leq 0, \end{aligned} \tag{39}$$

respectively. Then, by adopting Lemma 1, these constraints can be reformulated, respectively as

$$\begin{aligned} &\begin{bmatrix} \lambda_2 - \frac{\overline{P}_s}{P_p |g_e|^2 + \sigma_s^2} & -\frac{\overline{P}_s \hat{h}_e}{P_p |g_e|^2 + \sigma_s^2} \\ -\frac{\overline{P}_s \hat{h}_e}{P_p |g_e|^2 + \sigma_s^2} & 1 - \frac{\overline{P}_s |\hat{h}_s|^2}{P_p |g_e|^2 + \sigma_e^2} - t - \lambda_2 \epsilon_e^2 \end{bmatrix} \succeq \mathbf{0}, \\ &\lambda_2 \geq 0, \end{aligned} \tag{40}$$

and

$$\begin{aligned} &\begin{bmatrix} \lambda_3 - \overline{P}_s & -\overline{P}_s \hat{h}_p \\ -\overline{P}_s \hat{h}_p & tq - \overline{P}_s |\hat{h}_p|^2 + \sigma_s^2 - \lambda_e \epsilon_p^2 \end{bmatrix} \succeq \mathbf{0}, \\ &\lambda_3 \geq 0. \end{aligned} \tag{41}$$

This completes the proof of Proposition 1. ■

Appendix B
Proof of Proposition 2

In order to achieve a similar performance through the functions provided in (23) and (26), we should maximize the following likelihood function:

$$\begin{aligned} L(\mathbf{W}, \mathbf{b}) &= \prod_{m=1}^{M} p_m(y|x; \mathbf{W}, \mathbf{b}) \\ &= \prod_{m=1}^{M} \exp\left(- \frac{(f_m(\mathbf{S}, \mathbf{W}, \mathbf{b}) - P_{s,m}^*)^2}{2\sigma^2} \right). \end{aligned} \tag{42}$$

By utilizing the monotonicity of the logarithmic function, the logarithmic likelihood function can be expressed as

$$\begin{aligned} \log L(\mathbf{W}, \mathbf{b}) &= \log \prod_{m=1}^{M} \exp\left(- \frac{(f_m(\mathbf{S}, \mathbf{W}, \mathbf{b}) - P_{s,m}^*)^2}{2\sigma^2} \right) \\ &= M \log\left(\frac{1}{\sqrt{2\pi}\sigma} \right) - \frac{1}{2\sigma^2} \sum_{m=1}^{M} (f_m(\mathbf{S}, \mathbf{W}, \mathbf{b}) - P_{s,m}^*)^2. \end{aligned} \tag{43}$$

Since $M \log \frac{1}{\sqrt{2\pi}\sigma}$ and $\frac{1}{2\sigma^2}$ are constants, maximizing the likelihood function is equivalent to minimizing the following loss function:

$$J(\mathbf{W}, \mathbf{b}) = \sum_{m=1}^{M} (y_m - P_{s,m}^*)^2. \tag{44}$$

Furthermore, this loss function can be normalized without loss of generality as follows:

$$J(\mathbf{W}, \mathbf{b}) = \frac{1}{M} \sum_{m=1}^{M} (y_m - P_{s,m}^*)^2, \tag{45}$$

which completes the proof of Proposition 2. ■

APPENDIX C
PROOF OF PROPOSITION 3

First, we provide the following basic chain rule:

$$\frac{\partial h(g)}{\partial z} = \frac{\partial h}{\partial g}\frac{\partial g}{\partial z}. \tag{46}$$

From the feed-forward process, we have

$$\mathbf{z}^{(l+1)} = \mathbf{W}^{(l)}\mathbf{a}^{(l)} + \mathbf{b}^{(l)}, \tag{47}$$

$$\mathbf{a}^{(l+1)} = g(\mathbf{z}^{(l+1)}), \tag{48}$$

where $\mathbf{z}^{(l+1)}$ is the linear transformation of a given set of input parameters at the $(l+1)$-th layer, whereas $\mathbf{a}^{(l+1)}$ is the output activation value of the $(l+1)$-th layer. The function $g(\mathbf{z})$ represents the activation function. By assuming that $J(\mathbf{W}, \mathbf{b})$ is the loss function of the NN, we can write the following equations based on the chain rule defined in (46):

$$\begin{aligned}\frac{\partial J(\mathbf{W},\mathbf{b})}{\partial \mathbf{W}^{(l)}} &= \frac{\partial J(\mathbf{W},\mathbf{b})}{\partial \mathbf{z}^{(l+1)}}\frac{\partial \mathbf{z}^{(l+1)}}{\partial \mathbf{W}^{(l)}} \\ &= \frac{1}{M}\sum_{m=1}^{M}\boldsymbol{\delta}_m^{(l+1)}(\mathbf{a}_m^{(l)})^T,\end{aligned} \tag{49}$$

$$\frac{\partial J(\mathbf{W},\mathbf{b})}{\partial \mathbf{b}^{(l)}} = \frac{\partial J(\mathbf{W},\mathbf{b})}{\partial \mathbf{z}^{(l+1)}}\frac{\partial \mathbf{z}^{(l+1)}}{\partial \mathbf{b}^{(l)}} = \frac{1}{M}\sum_{m=1}^{M}\boldsymbol{\delta}_m^{(l+1)}. \tag{50}$$

Since we can calculate $\mathbf{a}_m^{(l)}$ from the feed-forward process, then $\boldsymbol{\delta}_m^{(l)}$ can be derived as follows. Based on the chain rule, we have

$$\begin{aligned}\boldsymbol{\delta}_m^{(l)} &= \frac{\partial J(\mathbf{W},\mathbf{b})}{\partial \mathbf{z}_m^{(l)}} = \frac{\partial J(\mathbf{W},\mathbf{b})}{\partial \mathbf{z}_m^{(l+1)}}\frac{\partial \mathbf{z}_m^{(l+1)}}{\partial \mathbf{a}_m^{(l)}}\frac{\partial \mathbf{a}_m^{(l)}}{\partial \mathbf{z}_m^{(l)}} \\ &= [(\mathbf{W}^{(l)})^T\boldsymbol{\delta}_m^{(l+1)}]\cdot g'(\mathbf{z}_m^{(l)}).\end{aligned} \tag{51}$$

Starting from the output layer, we can calculate $\boldsymbol{\delta}^{(l)}$ back forward layer-by-layer until the input layer. Finally, considering the gradient descent method, the weights matrix $\mathbf{W}^{(l)}$ and the bias vector $\mathbf{b}^{(l)}$ for the l-th layer can be updated respectively as follows:

$$\mathbf{W}^{(l)} = \mathbf{W}^{(l)} - \frac{\alpha}{M}\sum_{m=1}^{M}[\boldsymbol{\delta}_m^{(l+1)}(\mathbf{a}_m^{(l)})^T], \tag{52}$$

$$\mathbf{b}^{(l)} = \mathbf{b}^{(l)} - \frac{\alpha}{M}\sum_{m=1}^{M}\boldsymbol{\delta}_m^{(l+1)}, \tag{53}$$

which completes the proof of of Proposition 3. ■

REFERENCES

[1] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 63, no. 4, pp. 1678–1690, May. 2014.

[2] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Le Goff, "Robust outage secrecy rate optimizations for a MIMO secrecy channel," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 86–89, Feb. 2015.

[3] Z. Chu, H. Xing, M. Johnston, and S. Le Goff, "Secrecy rate optimizations for a MISO secrecy channel with multiple multi-antenna eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 283–297, Jan. 2016.

[4] M. Zhang, K. Cumanan, and A. G. Burr, "Secure energy efficiency optimization for MISO cognitive radio network with energy harvesting," in *Proc. IEEE WCSP*, Nanjing, Oct. 2017, pp. 1–6.

[5] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[6] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[7] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory.*, vol. 24, no. 3, pp. 339–348, May 1978.

[8] C. Jiang, H. Zhang, Y. Ren, Z. Han, K.-C. Chen, and L. Hanzo, "Machine learning paradigms for next-generation wireless networks," *IEEE Wireless Commun.*, vol. 24, no. 2, pp. 98–105, Apr. 2016.

[9] I. Goodfellow, Y. Bengio, and A. Courville, *Deep learning*. MIT Press Cambridge, 2016, vol. 1.

[10] C. Andrieu, N. De Freitas, A. Doucet, and M. I. Jordan, "An introduction to MCMC for machine learning," *Machine learning*, vol. 50, no. 1-2, pp. 5–43, Jan. 2003.

[11] F. Sebastiani, "Machine learning in automated text categorization," *ACM Computing Surveys*, vol. 34, no. 1, pp. 1–47, Mar. 2002.

[12] C. M. Bishop, *Pattern Recognition and Machine Learning*. Springer, 2006.

[13] J. W. Kalat, *Biological Psychology*. Nelson Education, 1995.

[14] M. Chen, U. Challita, W. Saad, C. Yin, and M. Debbah, "Machine learning for wireless networks with artificial intelligence: A tutorial on neural networks," *IEEE Commun. Surveys & Tutorials*, vol. 21, no. 4, pp. 3039–3071, Jul. 2019.

[15] H. B. Demuth, M. H. Beale, O. De Jess, and M. T. Hagan, *Neural Network Design*. Martin Hagan, 2014.

[16] T. Lin and Y. Zhu, "Beamforming design for large-scale antenna arrays using deep learning," *IEEE Wireless Commun. Lett.*, vol. 9, no. 1, Jan. 2020.

[17] H. Huang, Y. Song, J. Yang, G. Gui, and F. Adachi, "Deep-learning-based millimeter-wave massive MIMO for hybrid precoding," *IEEE Trans. Veh. Tech.*, vol. 68, no. 3, pp. 3027–3032, Mar. 2019.

[18] F. Zhou, G. Lu, M. Wen, Y. Liang, Z. Chu, and Y. Wang, "Dynamic spectrum management via machine learning: State of the art, taxonomy, challenges, and open research issues," *IEEE Network*, vol. 33, no. 4, Jul. 2019.

[19] C. Huang, G. C. Alexandropoulos, A. Zappone, C. Yuen, and M. Debbah, "Deep learning for UL/DL channel calibration in generic massive MIMO systems," in *Proc. ICC*, Shanghai, May 2019, pp. 1–6.

[20] M. Zhang, K. Cumanan, L. Ni, H. Hu, A. G. Burr, and Z. Ding, "Robust beamforming for AN aided MISO SWIPT system with unknown eavesdroppers and non-linear EH model," in *Proc. IEEE GLOBECOM WORKSHOP*, Abu Dhabi, Dec. 2018, pp. 1–7.

[21] K. Cumanan, H. Xing, P. Xu, G. Zheng, X. Dai, A. Nallanathan, Z. Ding, and G. K. Karagiannidis, "Physical layer security jamming: Theoretical limits and practical designs in wireless networks," *IEEE Access*, vol. 5, pp. 3603–3611, Dec. 2016.

[22] K. Cumanan, Z. Ding, M. Xu, and H. V. Poor, "Secrecy rate optimization for secure multicast communications," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1417–1432, Dec. 2016.

[23] Z. Chu, Z. Zhu, M. Johnston, and S. Y. Le Goff, "Simultaneous wireless information power transfer for MISO secrecy channel," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 6913–6925, Nov. 2016.

[24] Z. Chu, K. Cumanan, M. Xu, and Z. Ding, "Robust secrecy rate optimisations for multiuser multiple-input-single-output channel with device-to-device communications," *IET Commun.*, vol. 9, no. 3, pp. 396–403, Feb. 2015.

[25] M. Zeng, N. Nguyen, O. A. Dobre, and H. V. Poor, "Securing downlink massive MIMO-NOMA networks with artificial noise," *IEEE J. Sel. Signal Process.*, vol. 13, no. 3, pp. 685–699, Feb. 2019.

[26] H. Sun, X. Chen, Q. Shi, M. Hong, X. Fu, and N. D. Sidiropoulos, "Learning to optimize: Training deep neural networks for wireless resource management," in *Proc. IEEE SPAWC*, Sapporo, Jul. 2017, pp. 1–6.

[27] C. Zhang, P. Patras, and H. Haddadi, "Deep learning in mobile and wireless networking: A survey," *IEEE Commun. Surveys & Tutorials*, vol. 21, no. 3, pp. 2224– 2287, Mar. 2019.

[28] P. M. Domingos, "A few useful things to know about machine learning." *ACM Commun.*, vol. 55, no. 10, pp. 78–87, Spring 2012.

[29] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015.

[30] H. Ye, G. Y. Li, and B.-H. Juang, "Power of deep learning for channel estimation and signal detection in OFDM systems," *IEEE Wireless Commun. Lett.*, vol. 7, no. 1, pp. 114–117, Feb. 2018.

[31] C. Huang, G. C. Alexandropoulos, C. Yuen, and M. Debbah, "Indoor signal focusing with deep learning designed reconfigurable intelligent surfaces," in *Proc. IEEE SPAWC*. IEEE, Cannes, Jul. 2019, pp. 1–5.

[32] C. Huang, R. Mo, and C. Yuen, "Reconfigurable intelligent surface assisted multiuser MISO systems exploiting deep reinforcement learning," *IEEE J. Sel. Commun.*, vol. 38, no. 8, pp. 1839 – 1850, Aug. 2020.

[33] F. Zhou, X. Zhang, R. Q. Hu, A. Papathanassiou, and W. Meng, "Resource allocation based on deep neural networks for cognitive radio networks," in *Proc. IEEE ICCC*, Beijing, Feb. 2018, pp. 40–45.

[34] H. Ye and G. Y. Li, "Deep reinforcement learning for resource allocation in V2V communications," in *Proc. IEEE ICC*, Kansas City, May 2018, pp. 1–6.

[35] H. Sun, X. Chen, Q. Shi, M. Hong, X. Fu, and N. D. Sidiropoulos, "Learning to optimize: Training deep neural networks for interference management," *IEEE Trans. Signal Process.*, vol. 66, no. 20, pp. 5438–5453, Oct. 2018.

[36] C. Huang, G. C. Alexandropoulos, A. Zappone, C. Yuen, and M. Debbah, "Deep learning for UL/DL channel calibration in generic massive MIMO systems," in *Proc. IEEE ICC*, Shanghai, May 2019, pp. 1–6.

[37] Y. Sun, J. Liu, J. Wang, Y. Cao, and N. Kato, "When machine learning meets privacy in 6g: A survey," *IEEE Communications Surveys & Tutorials*, Early Access 2020.

[38] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of things (IoT) security," *IEEE Communications Surveys & Tutorials*, Thirdquarter 2020.

[39] T. O'Shea and J. Hoydis, "An introduction to deep learning for the physical layer," *IEEE Trans. Cognitive Commun. & Network.*, vol. 3, no. 4, pp. 563–575, Dec. 2017.

[40] M. Zhang, K. Cumanan, and A. G. Burr, "Secrecy rate maximization for MISO multicasting SWIPT system with power splitting scheme," in *Proc. IEEE SPAWC*, Edinburgh, Jul. 2016, pp. 1–5.

[41] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, "Secure communications with cooperative jamming: Optimal power allocation and secrecy outage analysis," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7495–7505, Aug. 2017.

[42] A. Charnes and W. W. Cooper, "Programming with linear fractional functionals," *Naval Res. Logist. Quart.*, vol. 9, no. 3-4, pp. 181–186, 1962.

[43] S. P. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory*. SIAM, 1994, vol. 15.

[44] S. Shahbazpanahi, A. B. Gershman, Zhi-Quan Luo, and Kon Max Wong, "Robust adaptive beamforming using worst-case sinr optimization: a new diagonal loading-type solution for general-rank signal models," in *Proc. IEEE ICASSP*, vol. 5, Hong Kong, Apr. 2003, pp. V–333.

[45] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, "Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3472–3482, Nov. 2012.

[46] A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the MIMO wiretap channel," in *Proc. IEEE ICASSP*, Kyoto, Mar. 2012, pp. 2809–2812.

[47] Y. Guo and B. C. Levy, "Worst-case MSE precoder design for imperfectly known MIMO communications channels," *IEEE Trans. Signal Process.*, vol. 53, no. 8, pp. 2918–2930, Aug. 2005.

[48] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[49] K. Hornik, M. Stinchcombe, H. White *et al.*, "Multilayer feedforward networks are universal approximators." *Neural networks*, vol. 2, no. 5, pp. 359–366, 1989.

[50] S. Reed and N. De Freitas, "Neural programmer-interpreters," *arXiv preprint arXiv:1511.06279*, 2015.

[51] J. Luo, J. Tang, D. K. C. So, G. Chen, K. Cumanan, and J. A. Chambers, "A deep learning-based approach to power minimization in multi-carrier NOMA with SWIPT," *IEEE Access*, vol. 7, pp. 17 450–17 460, Jan. 2019.

[52] C. Jiang, H. Zhang, Y. Ren, Z. Han, K.-C. Chen, and L. Hanzo, "Machine learning paradigms for next-generation wireless networks," *IEEE Wireless Commun.*, vol. 24, no. 2, pp. 98–105, Apr. 2017.

[53] A. Hirose, *Complex-valued Neural Networks: Advances and Applications*. John Wiley & Sons, 2013, vol. 18.

[54] D. J. Leinweber, "Stupid data miner tricks: overfitting the s&p 500," *The Journal of Investing*, vol. 16, no. 1, pp. 15–22, Spring 2007.

[55] D. Chicco, "Ten quick tips for machine learning in computational biology," *BioData Mining*, vol. 10, no. 1, p. 35, Dec. 2017.

[56] Y. Bengio, F. Bastien, A. Bergeron, N. Boulanger-Lewandowski, T. Breuel, Y. Chherawala, M. Cisse, M. Côté, D. Erhan, J. Eustache, X. Glorot, X. Muller, S. P. Lebeuf, R. Pascanu, S. Rifai, F. Savard, and G. Sicard, "Deep learners benefit more from out-of-distribution examples," in *Proc. JMLR AISTATS*, Fort Lauderdale, Apr. 2011, pp. 164–172.

[57] F. Girosi, M. Jones, and T. Poggio, "Regularization theory and neural networks architectures," *Neural Computation*, vol. 7, no. 2, pp. 219–269, Mar. 1995.

[58] L. Wang, M. D. Gordon, and J. Zhu, "Regularized least absolute deviations regression and an efficient algorithm for parameter tuning," in *Proc. IEEE ICDM*, Hong Kong, Dec. 2006, pp. 690–700.

[59] A. E. Hoerl and R. W. Kennard, "Ridge regression: biased estimation for nonorthogonal problems," *Technometrics*, vol. 42, no. 1, pp. 80–86, Feb. 2000.

[60] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," *arXiv preprint arXiv:1412.6980*, 2014.

[61] X. Glorot and Y. Bengio, "Understanding the difficulty of training deep feedforward neural networks," in *Proc, ICAIS*, Sardinia, 2010, pp. 249–256.

[62] L. N. Smith, "Cyclical learning rates for training neural networks," in *Proc. IEEE WACV*, Santa Rosa, Mar. 2017, pp. 464–472.

[63] I. V. Tetko, D. J. Livingstone, and A. I. Luik, "Neural network studies. 1. comparison of overfitting and overtraining," *J. Chem. Inf. Comput. Sci.*, vol. 35, no. 5, pp. 826–833, Jan. 1995.

[64] T. Li, M. R. A. Khandaker, F. Tariq, K. Wong, and R. T. Khan, "Learning the wireless V2I channels using deep neural networks," in *Proc. IEEE VTC-Fall*, Honolulu, Sep. 2019, pp. 1–5.

[65] H. Lee, S. H. Lee, and T. Q. S. Quek, "Deep learning for distributed optimization: Applications to wireless resource management," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 10, pp. 2251–2266, Oct. 2019.